Manipulationssichere Erzeugung von echten Zufallszahlen

Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zur Erzeugung einer echten Zufallszahl.

Beispielsweise für Zugriffsschutz- oder Verschlüsselungszwecke ist es erforderlich, gute manipulationssichere Zufallszahlen zu erzeugen. Im Zusammenhang mit Kraftfahrzeugwegfahrsperren erfolgt diese Erzeugung der Zufallszahlen beispielsweise auf der Ebene der Motorsteuerung, bei der es sich in vielen Fällen um ein Embedded-System handelt. Dabei scheidet der Einsatz von externen Quellen aufgrund von Manipulationsmöglichkeiten und die Verwendung von speziellen Schaltkreisen wegen der damit verbundenen zusätzlichen Stückkosten aus.

Zur Erzeugung echter Zufallszahlen ist es unter anderem bekannt, die niederwertigen Bits einer A/D-Wandlung von Signalen einer separaten Rauschquelle zu verwenden, was jedoch mit erheblichen Kosten verbunden ist. Es ist ebenfalls bekannt, eine echte Zufallszahl über eine Zeitmessung eines externen Ereignisses, beispielsweise der Dauer eines vom Benutzer vorgenommenen Tastendruckes, zu erzeugen. Diese Lösung scheidet jedoch zumindest in den Fällen aus, in denen das System die Kommunikation eröffnet und daher vor einem externen Ereignis die Zufallszahl erzeugen muss. Neben der Erzeugung von echten Zufallszahlen ist es weiterhin bekannt, eine Pseudo-Zufallszahlenreihe zu nutzen und den aktuellen Status beispielsweise in einem nicht-flüchtigen Speicher des Systems zu speichern. Allerdings ist die Qualität von Pseudo-Zufallszahlen im Vergleich zu echten Zufallszahlen unzureichend.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren sowie eine Vorrichtung anzugeben, mit denen eine echte Zufallszahl schnell, das heißt beispielsweise im Millisekundenbereich, speichersparend, gerätelaufzeitunabhängig, ohne Speicherung zwischen den Betriebszyklen des Steuergeräts und ohne externe Quellen (zufällige Trigger) erzeugt werden können.

Diese Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst.

Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Das erfindungsgemäße Verfahren baut auf dem gattungsgemäßen Stand der Technik dadurch auf, dass die echte Zufallszahl auf der Grundlage einer stochastisch verteilten Dauer eines elektrischen Umladevorgangs erzeugt wird. Durch diese Lösung wird eine echte Zufallszahl erzeugt, das heißt keine Pseudo-Zufallszahl. Weiterhin kann das Verfahren nicht durch externe Beschaltung manipuliert werden. In vielen Fällen werden gegenüber der vorhandenen Bestückung des jeweiligen Systems keine weiteren Bauteile benötigt, so dass die Zusatzkosten gering sind. Ein weiterer Vorteil des erfindungsgemäßen Verfahrens besteht darin, dass es nicht erforderlich ist, einen Zustand zu speichern, der dann manipuliert beziehungsweise zurückgesetzt werden könnte. Das erfindungsgemäße Verfahren ist besonders vorteilhaft, wenn der die stochastische Quelle bildende Umladevorgang in einer Komponente durchgeführt werden kann, die ohnehin Bestandteil des Systems ist, das neben der Erfüllung anderer Aufgaben auch die Zufallszahl erzeugen muss.

Bei bevorzugten Ausführungsformen des erfindungsgemäßen Verfahrens ist vorgesehen, dass der Umladevorgang ein Umladen zumindest einer Speicherzelle umfasst. Speicherzellen sind ohnehin Bestandteil moderner Systeme und stellen daher eine besonders kostengünstige Grundlage zur Durchführung des Umladevorgangs dar.

In diesem Zusammenhang kann beispielsweise vorgesehen sein, dass zumindest eine Speicherzelle eine Speicherzelle eines EEPROM ist. Die Dauer eines Umladevorgangs einer EEPROM-Speicherzelle unterliegt vergleichsweise großen stochastischen Streuungen, auf deren Grundlage sich echte Zufallszahlen erzeugen lassen.

Alternativ ist es ebenfalls möglich, dass zumindest eine Speicherzelle eine Speicherzelle eines FLASH-Speichers ist. FLASH-Speicher finden zunehmend Verwendung und stellen daher in vielen Fällen ohne zusätzliche Kosten eine geeignete Grundlage für die erfindungsgemäße Erzeugung von echten Zufallszahlen dar.

Bei bevorzugten Ausführungsformen des erfindungsgemäßen Verfahrens ist weiterhin vorgesehen, dass der Umladevorgang mit Hilfe einer Ladungspumpe durchgeführt wird. Der Einsatz von Ladungspumpen ist beispielsweise im Zusammenhang mit EEPROMs üblich, wobei in vielen Fällen On-Chip-Ladungspumpen vorgesehen sind.

Bei dem erfindungsgemäßen Verfahren kann in vorteilhafter Weise weiterhin vorgesehen sein, dass die stochastische Dauer des Umladevorgangs mit Hilfe eines Zählers erfasst wird. Dabei ist es vorteilhaft, wenn die Taktung des Zählers möglichst hoch ist, so dass sich hinsichtlich des als Grundlage

für die Zufallszahl dienenden Zählerstandes am Ende des Umladevorgangs möglichst große Streuungen ergeben.

Das erfindungsgemäße Verfahren wird als besonders vorteilhaft erachtet, wenn vorgesehen ist, dass es von einem Embedded-System durchgeführt wird, insbesondere von einer Motorsteuerung eines Kraftfahrzeugs. Dabei kommen prinzipiell alle Embedded-Systems in Frage, die in Umgebungen eingesetzt werden, in denen (auch) die Erzeugung von guten Zufallszahlen erforderlich ist.

Die erfindungsgemäße Vorrichtung baut auf dem gattungsgemäßen Stand der Technik dadurch auf, dass sie die echte Zufallszahl auf der Grundlage einer stochastisch verteilten Dauer eines elektrischen Umladevorgangs erzeugt. Dadurch ergeben sich die im Zusammenhang mit dem erfindungsgemäßen Verfahren erläuterten Vorteile und Eigenschaften in gleicher oder ähnlicher Weise, weshalb zur Vermeidung von Wiederholungen auf die entsprechenden obigen Ausführungen verwiesen wird.

Gleiches gilt sinngemäß für die nachfolgend angegebenen vorteilhaften Weiterbildungen der erfindungsgemäßen Vorrichtung, wobei auch diesbezüglich auf die entsprechenden Ausführungen im Zusammenhang mit dem erfindungsgemäßen Verfahren verwiesen wird.

Die erfindungsgemäße Vorrichtung ist in vorteilhafter Weise dadurch weitergebildet, dass sie zumindest eine Speicherzelle aufweist, die zur Erzeugung der Zufallszahl elektrisch umgeladen wird.

Dabei kann in vorteilhafter Weise vorgesehen sein, dass zumindest eine Speicherzelle eine Speicherzelle eines EEPROM ist.

Zusätzlich oder alternativ ist es möglich, dass zumindest eine Speicherzelle eine Speicherzelle eines FLASH-Speichers ist.

Die erfindungsgemäße Vorrichtung ist in vorteilhafter Weise dadurch weitergebildet, dass sie zur Durchführung des Umladevorgangs eine Ladungspumpe aufweist.

Im Zusammenhang mit der erfindungsgemäßen Vorrichtung kann weiterhin vorgesehen sein, dass sie zur Erfassung der stochastisch verteilten Dauer des Umladevorgangs einen Zähler aufweist.

Als besonders vorteilhaft werden Ausführungsformen der erfindungsgemäßen Vorrichtung erachtet, bei denen vorgesehen ist, dass sie ein Embedded-System ist, insbesondere eine Motorsteuerung eines Kraftfahrzeugs.

Ein wesentlicher Grundgedanke der vorliegenden Erfindung besteht darin, dass echte Zufallszahlen praktisch ohne Mehrkosten von Systemen erzeugt werden können, wenn als stochastische Quelle eine ohnehin zum System zählende Komponente verwendet wird, beispielsweise eine Ladungspumpe, die Bestandteil eines Steuergeräts ist. Die Erfindung eignet sich insbesondere für alle Dienststellen, die mit vorhandenen Systemen (das heißt ohne extra dafür vorgesehene Bauteile) eine gute, echte Zufallszahl erzeugen müssen, ohne Zugriff auf unabhängige, manipulationssichere Generatoren (Trigger) zu haben. Darunter fallen, ohne darauf beschränkt zu sein, insbesondere

alle kostenoptimierten Embedded-Systems. Im Zusammenhang mit der Kraftfahrzeugtechnik werden Zufallszahlen beispielsweise insbesondere für den Zugriffsschutz (auch bei Wartungsarbeiten) und für Verschlüsselungszwecke (zum Beispiel Wegfahrsperre) benötigt.

Ausführungsformen der Erfindung werden nachfolgend anhand der zugehörigen Zeichnungen beispielhaft erläutert.

Es zeigen:

Figur 1 ein Flussdiagramm, das eine Ausführungsform des erfindungsgemäßen Verfahrens veranschaulicht;

Figur 2 einen Graph, der mögliche Umladevorgänge einer Speicherzelle veranschaulicht;

Figur 3 ein stark vereinfachtes, schematisches Blockschaltbild von Komponenten einer Motorsteuerung.

Die in Figur 1 dargestellte Ausführungsform des erfindungsgemäßen Verfahrens beginnt beim Schritt S1. Im Schritt S2 wird ein Zähler zurückgesetzt, dessen späterer Zählerstand als Grundlage für die Erzeugung der echten Zufallszahl dient oder der diese Zufallszahl direkt darstellt. Im Schritt S3 wird ein Umladevorgang begonnen und gleichzeitig der Zähler gestartet. Bei dem Umladevorgang kann es sich insbesondere um ein Schreiben in eine EEPROM- oder FLASH-Speicherzelle handeln, das üblicherweise unter Verwendung einer Ladungspumpe erfolgt. Im Schritt S4 wird solange geprüft, ob der Umladevorgang abgeschlossen ist, bis dies der Fall ist. Anschließend wird im Schritt S5 der Zähler gestoppt. Im Schritt S6 wird der Zählerstand ausgelesen und als echte Zufallszahl

verwendet. Gegebenenfalls kann die endgültige Zufallszahl jedoch auch unter Zuhilfenahme weiterer Rechenfunktion erzeugt werden. Das dargestellte Verfahren endet im Schritt S7.

Figur 2 veranschaulicht drei stochastisch verteilte Umladevorgänge einer Speicherzelle. Die tatsächliche Dauer eines aktuellen Umladevorgangs kann dabei zwischen einer kürzesten Dauer T' (Kurve Q') und einer längsten Dauer T'' (Kurve Q'') liegen und beispielsweise T (Kurve Q) betragen.

Figur 3 zeigt ein stark vereinfachtes, schematisches Blockschaltbild von Komponenten einer Motorsteuerung, wobei die dargestellte Motorsteuerung 18 in Form eines Embedded-Systems vorliegt. Die Motorsteuerung 18 kann eine Vielzahl weiterer nicht dargestellter Komponenten umfassen, die zur Erfüllung aller an die Motorsteuerung gestellten Aufgaben erforderlich sind. Sämtliche im Folgenden näher erläuterten Komponenten sind ohnehin Bestandteil der Motorsteuerung 18, das heißt nicht speziell zur Erzeugung der echten Zufallszahlen vorgesehen. Die dargestellte Motorsteuerung 18 weist einen intelligenten Controller 20 auf, der unter anderem dazu geeignet ist, eine Ladungspumpe 14 anzusteuern, die dazu vorgesehen ist, eine Speicherzelle 10 eines Speicherzellenarrays 22 eines EEPROMs 12 umzuladen, wenn der Inhalt der Speicherzelle 10 verändert werden soll. Der Controller 20 kommuniziert weiterhin mit einem Zähler 16, mit dem die tatsächliche Dauer eines Umladevorgangs der Speicherzelle 10 erfasst wird. Der Fachmann erkennt, dass mit den in Figur 3 dargestellten Komponenten das anhand von Figur 1 erläuterte Verfahren in vorteilhafter Weise durchgeführt werden kann. Auf eine erneute Erläuterung des Ablaufs der Erzeugung einer Zufallszahl wird daher an dieser Stelle verzichtet.

Die in der vorstehenden Beschreibung, in den Zeichnungen sowie in den Ansprüchen offenbarten Merkmale der Erfindung können sowohl einzeln als auch in beliebiger Kombination für die Verwirklichung der Erfindung wesentlich sein.

Patentansprüche

1. Verfahren zum Erzeugen einer echten Zufallszahl, dadurch gekennzeichnet, dass die echte Zufallszahl auf der Grundlage einer stochastisch verteilten Dauer (T) eines elektrischen Umladevorgangs erzeugt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Umladevorgang ein Umladen zumindest einer Speicherzelle (10) umfasst.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass zumindest eine Speicherzelle (10) eine Speicherzelle eines EEPROM (12) ist.

4. Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, dass zumindest eine Speicherzelle (10) eine Speicherzelle eines FLASH-Speichers ist.

5. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass der Umladevorgang mit Hilfe einer Ladungspumpe (14) durchgeführt wird.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die stochastische Dauer (T) des Umladevorgangs mit Hilfe eines Zählers (16) erfasst wird.

7. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass es von einem Embedded-System (18) durchgeführt wird, insbesondere von einer Motorsteuerung (18) eines Kraftfahrzeugs.

8. Vorrichtung, die zur Erzeugung einer echten Zufallszahl geeignet ist, dadurch gekennzeichnet, dass sie die echte Zufallszahl auf der Grundlage einer stochastisch verteilten Dauer (T) eines elektrischen Umladevorgangs erzeugt.

9. Vorrichtung nach Anspruch 8, dadurch gekennzeichnet, dass sie zumindest eine Speicherzelle (10) aufweist, die zur Erzeugung der Zufallszahl elektrisch umgeladen wird.

10. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, dass zumindest eine Speicherzelle (10) eine Speicherzelle eines EEPROM (12) ist.

11. Vorrichtung nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass zumindest eine Speicherzelle (10) eine Speicherzelle eines FLASH-Speichers ist.

12. Vorrichtung nach einem der Ansprüche 8 bis 11, dadurch gekennzeichnet, dass sie zur Durchführung des Umladevorgangs eine Ladungspumpe (14) aufweist.

13. Vorrichtung nach einem der Ansprüche 8 bis 12, dadurch gekennzeichnet, dass sie zur Erfassung der stochastisch verteilten Dauer (T) des Umladevorgangs einen Zähler (16) aufweist.

14. Vorrichtung nach einem der Ansprüche 8 bis 13, dadurch gekennzeichnet, dass sie ein Embedded-System (18) ist, insbesondere eine Motorsteuerung (18) eines Kraftfahrzeugs.

FIG 1

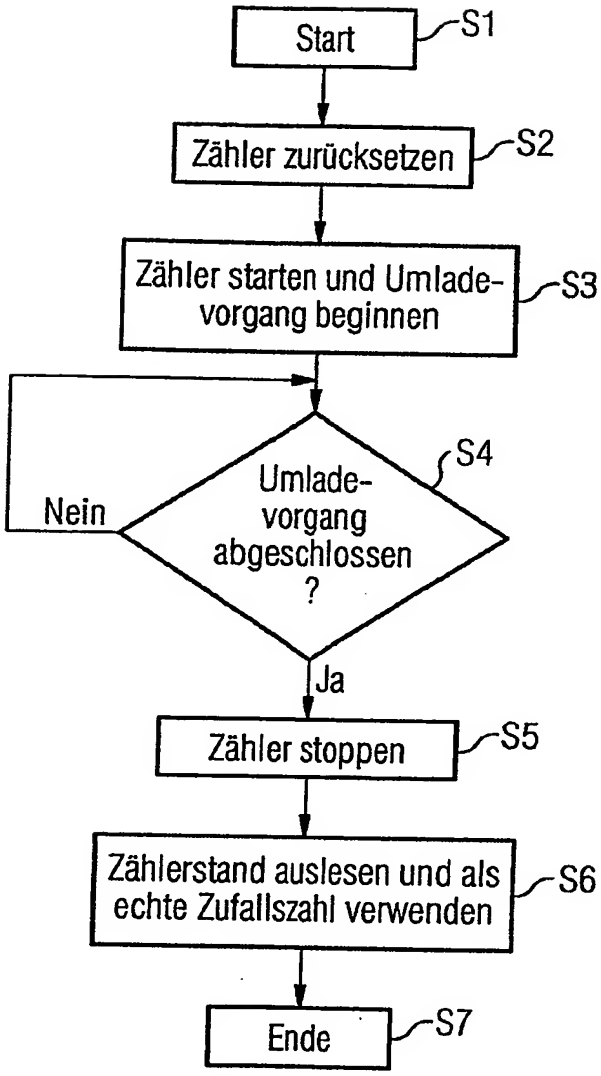

Start
S1
Zähler zurücksetzen
S2
Zähler starten und Umlade-vorgang beginnen
S3
Umlade-vorgang abgeschlossen ?
S4
Nein
Ja
Zähler stoppen
S5
Zählerstand auslesen und als echte Zufallszahl verwenden
S6
Ende
S7

FIG 2

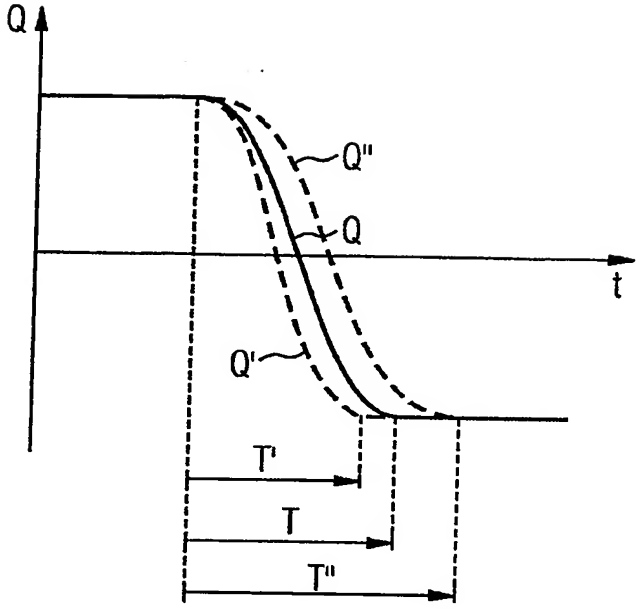
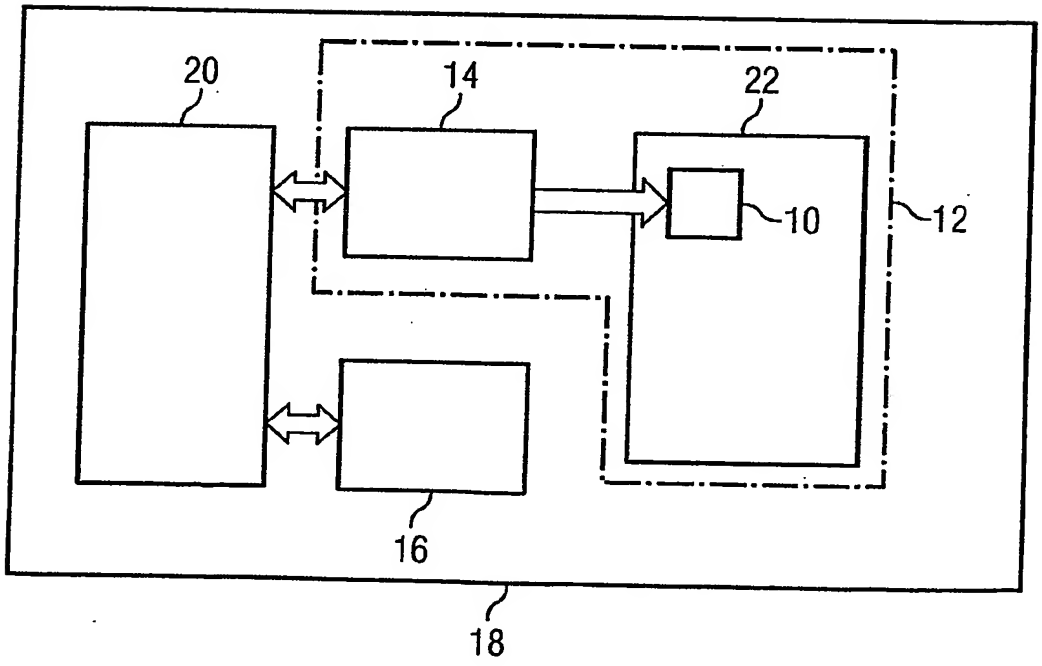


FIG 3



INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/050453

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H03K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	EP 1 513 061 A (INFINEON TECHNOLOGIES AG) 9 March 2005 (2005-03-09) abstract column 3, line 56 - column 4, line 38 column 5, line 11 - line 14 figures 1-3	1,2,8,9
A	EP 1 341 079 A (KABUSHIKI KAISHA TOSHIBA) 3 September 2003 (2003-09-03) abstract column 4, line 3 - line 52 figure 1	1-14
A	DE 101 00 346 A1 (SIEMENS AG) 11 July 2002 (2002-07-11) abstract column 1, line 64 - column 2, line 17	1-14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 May 2005	14/06/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Post, K

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2005/050453

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1513061 A	09-03-2005	EP 1513061 A1	09-03-2005
EP 1341079 A	03-09-2003	JP 2003258240 A	12-09-2003
		EP 1341079 A2	03-09-2003
		US 2003162587 A1	28-08-2003
DE 10100346 A1	11-07-2002	WO 02054807 A1	11-07-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/050453

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F7/58

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F H03K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, INSPEC, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
E	EP 1 513 061 A (INFINEON TECHNOLOGIES AG) 9. März 2005 (2005-03-09) Zusammenfassung Spalte 3, Zeile 56 - Spalte 4, Zeile 38 Spalte 5, Zeile 11 - Zeile 14 Abbildungen 1-3	1,2,8,9
A	EP 1 341 079 A (KABUSHIKI KAISHA TOSHIBA) 3. September 2003 (2003-09-03) Zusammenfassung Spalte 4, Zeile 3 - Zeile 52 Abbildung 1	1-14
A	DE 101 00 346 A1 (SIEMENS AG) 11. Juli 2002 (2002-07-11) Zusammenfassung Spalte 1, Zeile 64 - Spalte 2, Zeile 17	1-14

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
25. Mai 2005	14/06/2005

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Post, K

Formblatt PCT/ISA/210 (Blatt 2) (Januar 2004)

INTERNATIONAL[redacted] RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inte[redacted]nales Aktenzeichen
PCT/EP2005/050453

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie			Datum der Veröffentlichung
EP 1513061	A	09-03-2005	EP	1513061	A1	09-03-2005
EP 1341079	A	03-09-2003	JP	2003258240	A	12-09-2003
			EP	1341079	A2	03-09-2003
			US	2003162587	A1	28-08-2003
DE 10100346	A1	11-07-2002	WO	02054807	A1	11-07-2002